

# Networks and Network Devices: Communicating and Connecting

Dr. Jian-Ren Hou

# How Do You Interact with a Network

- A **Network** is a system of two or more devices linked by wires, cables, or a telecommunications system.
- **Networks** allow computers to share resources, such as hardware, software, data, and information.
- A **Network** requires a combination of hardware and software to operate.
- **Networks** act as a communications system around the globe through the Internet.

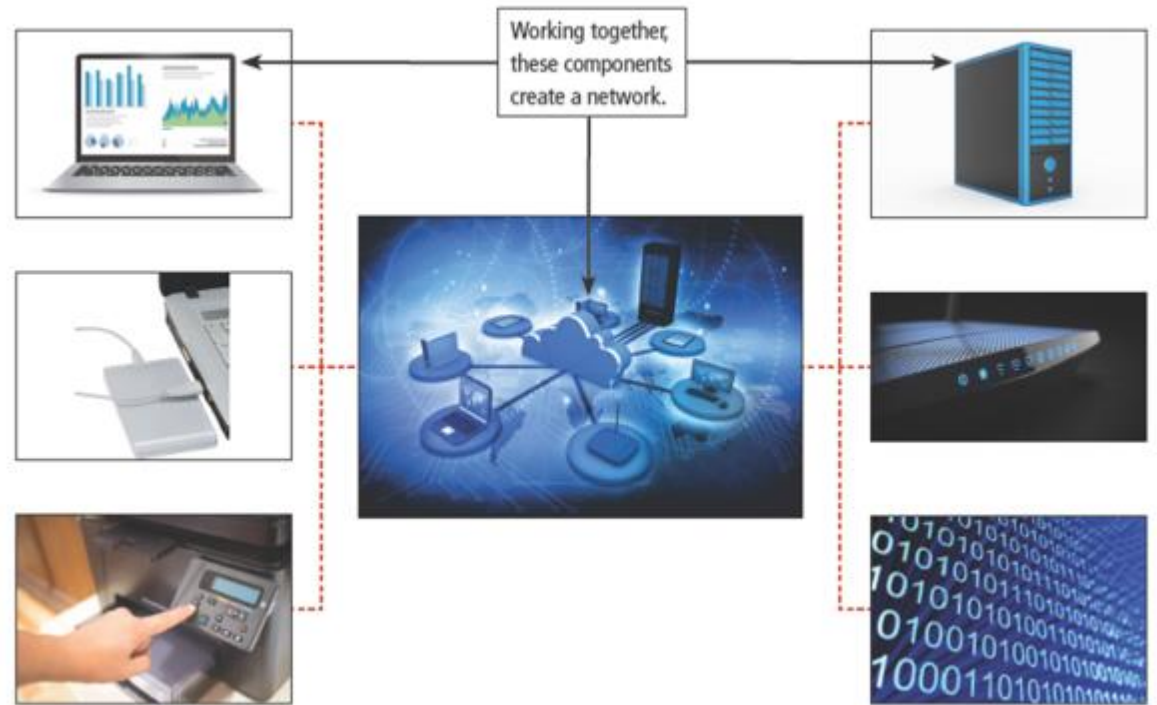


Figure 9-1 Networks can share resources and data

# How Do You Interact with a Network

- The process in which two or more computers or devices transfer data, instructions, and information is known as **digital communications**.
- All types of computers and mobile devices serve as sending and receiving devices in a **communications system**.
- Communications devices are modems, wireless access points, routers, and so on.
- Transmission media can be wired or wireless.

# How Do You Interact with a Network



Figure 9-3 Typical home network.

# How Do You Interact with a Network

**Home Networks** provide home users with the following capabilities:

- Multiple users can share a single Internet connection.
- Files on each computer, such as photos, can be shared.
- Multiple computers can share a single hardware resource, such as a printer.
- Game consoles can connect to the Internet to facilitate online gaming.

**Business Networks** provide the following advantages to businesses:

- Facilitate communication among employees
- Share hardware, such as printers and scanners
- Share data, information, and software with one another
- Centrally store and backup critical information

# How Do You Interact with a Network

- Businesses use intranets, extranets, and VPNs (virtual private networks) to provide different services to employees.

## Intranet

An **intranet** (intra means within) is an internal network that uses Internet technologies.

## Extranet

An **extranet** (extra means outside or beyond) allows customers or suppliers to access part of its intranet.

## VPN

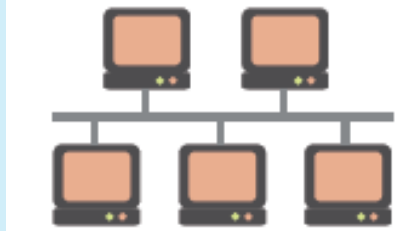
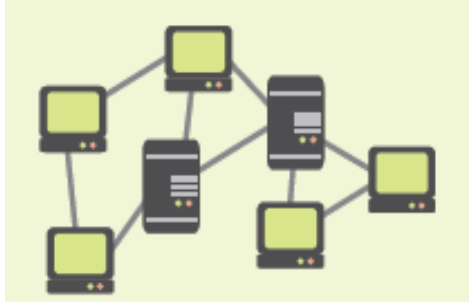
A **VPN** can allow an individual to access an organization's network by using encryption and other technologies to secure the data transmitted along the path.

# Network Structures

- Home and business networks describe the main users of a **Network**.
- **Networks** can be classified by:
  - ✓ Their **topology** (the method by which computers and devices are physically arranged on a network)
  - ✓ **Network architecture** (the logical design of all devices on a network)
  - ✓ Geographic reach
- **Topology** describes the layout of network devices, **architecture** describes the role of servers and users, and the geographic span of a network determines how wide the network reaches.
- Common network topologies include bus network, ring network, star network, and mesh network.

# Network Structures

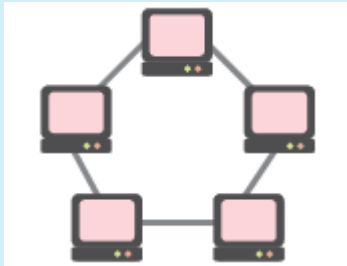

**Table 9-2 Network topologies.**

Type	Description	Layout
Bus network	All devices are attached to a central cable, called a “bus,” that carries the data. If the bus fails, the devices on the network will no longer be able to communicate.	
Mesh network	All devices are interconnected with one another. If a single device on the network fails, the rest of the network will continue to function by communicating via an alternate route. Two types of mesh topologies are a <b>full mesh topology</b> (each device on the network is connected to every other device on the network) and a <b>partial mesh technology</b> (each device may or may not be connected to all other devices on the network).	



# Network Structures

**Table 9-2 Network topologies (continued).**

Type	Description	Layout
Ring network	Data travels from one device to the next in a sequential fashion. If one device on the network fails, all communication on the network could cease to function. Ring networks are no longer common.	
Star network	Each device on the network is attached to a central device, such as a server or switch. If the central device fails, the other devices will be unable to communicate. If a connected device fails, all other devices will still be able to communicate. Two or more star networks may be joined together using a bus to form a tree topology. Tree topologies are often used in schools and businesses.	

# Network Structures

- On a **client/server network**, one or more computers act as a server, and the other computers on the network request resources from the server.
- A **client** is a computer or mobile device on the network that relies on the server for its resources.
- **Client/server networks** are controlled by a network administrator.



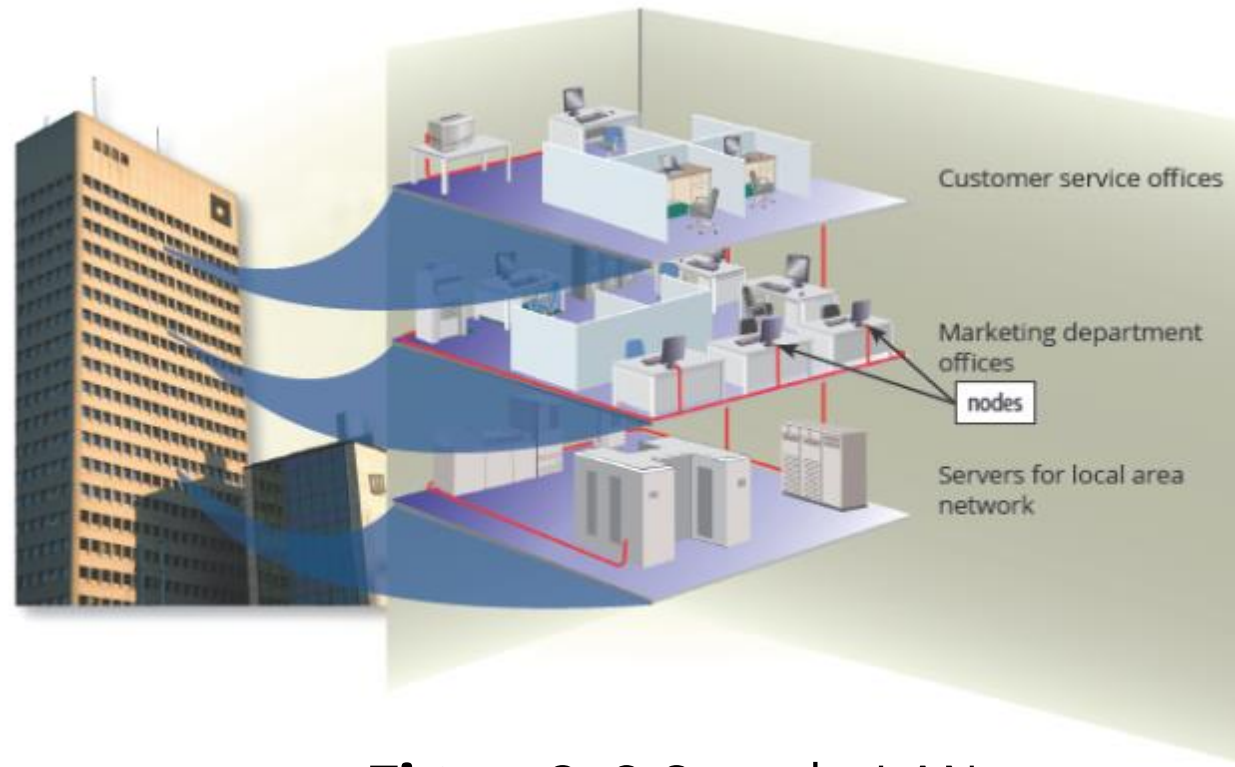
**Figure 9-5** Sample client/server network.

# Network Structures

- A **peer-to-peer (P2P) network** is a network architecture that connects a small number of computers, fewer than 10.
- With this type of **network**, computers communicate directly with one another and can share one another's resources.
- All computers are treated equally, and a network administrator is not required.
- A type of **P2P network** where users share files over the Internet.
- The files in an **Internet peer-to-peer** network transfer directly from one user's computer to the other.
- It is illegal to share copyright-protected files or other resources.

# Network Structures

- A **local area network (LAN)** connects computers and devices in a limited area.



**Figure 9-6** Sample LAN.

# Network Structures

- **Network configurations** come in a variety of sizes, which can be determined not only by the number of devices they connect but also by their geographic reach.
- A **wireless LAN (WLAN)** is a LAN that uses wireless connections.
- A **wide area network (WAN)** is a network that connects devices in a large geographic region.
- A **metropolitan area network (MAN)** is a type of wide-area network that is operated by a city or county.
- A **personal area network (PAN)** connects personal digital devices connected via Bluetooth like a smartwatch.
- A **body area network (BAN)** is a form of personal area network that consists of small, lightweight biosensors implanted in the body.

# Network Standards and Protocols

- **Network standards** define guidelines that specify the way computers access a network, the type(s) of hardware used, data transmission speeds, and the types of cable and wireless technology used.
- Network standards and protocols work together to move data through a network.
- The most common standard for wired networks is **Ethernet**. It controls how network interface cards (NICs), routers, and modems share access to cables and phone lines, as well as how they transmit data.
- Most businesses use a standard, such as **EDI (electronic data interchange)**, that defines how business documents travel across transmission media.

# Network Standards and Protocols

- A **protocol** may define data format, coding schemes, error handling, and the sequence in which data transfers over a network.
- One common family of protocols is **TCP/IP (Transmission Control Protocol/Internet Protocol)**.
- **TCP** defines how data is routed through a network, and **IP** specifies that all computers and devices connected to a network have a unique IP address.
- Two types of IP addresses: **IPv4** (Internet Protocol version 4) and **IPv6** (Internet Protocol version 6).

# Network Standards and Protocols

- **Wireless capability** of computers or devices to communicate via radio waves with other computers or devices using Wi-Fi, which identifies any network based on the 802.11 standards.
- **802.11** is a series of network standards developed by the IEEE.
- **Common standards** include 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax, with data transfer rates ranging from 11 Mbps to 7 Gbps.
- A designation of **802.11 a/b/g/n/ac/ax/be** on a computer, router, or other device indicates that it supports those six standards.
- Wi-Fi networks can easily be integrated with wired Ethernet networks.
- Extra hardware needs to be installed to extend or strengthen a wireless signal.



# Network Standards and Protocols

- **Bluetooth** is a network protocol that defines how two Bluetooth devices use short-range radio waves to transmit data.
- The data transfers between devices at a lower rate than WiFi.
- A **Bluetooth** device contains a small chip that allows it to communicate with other Bluetooth devices.
- Two **Bluetooth** devices are connected initially using a code, and devices that share a **Bluetooth connection** are said to be paired.
- Connect devices with vehicle stereos to use the vehicle's speakers to project sound
- Use GPS receivers to send directions to a mobile phone or GPS-enabled device
- Transfer photos wirelessly from a digital camera to a laptop or server. Replace wired communications devices, such as barcode readers, with wireless devices to enhance portability

# Network Standards and Protocols

- **UWB (Ultra-wideband)** is a network standard that specifies how two **UWB** devices use short-range radio waves to communicate at high speeds with each other.
- High Accuracy.
- **UWB** can transmit signals through doors and other obstacles.
- **UWB** is best suited for the transmission of large files, such as video, graphics, and audio.
- **Examples of UWB** uses include locating and tracking inventory, equipment, or personnel in remote or dangerous areas.
- Devices, such as television remote controls, use the **IrDA (Infrared Data Association)** standard to transmit data wirelessly to each other via infrared (IR) light waves.
- Since **Bluetooth and UWB** do not require line-of-sight transmission, these technologies are more widespread than IrDA.

# Network Standards and Protocols

- **RFID (radio frequency identification)** is a protocol that defines how a network uses radio signals to communicate with a **tag** placed in or attached to an object, an animal, or a person.
- The **tag**, called a transponder, consists of an antenna and a memory chip that contains the information to be transmitted.
- An RFID reader, also called a transceiver, reads the radio signals and transfers the information to a computer or other computing device.
- Readers can be handheld or embedded in an object, such as a doorway or a tollbooth.

# Network Standards and Protocols

- **NFC (near-field communications)** is a protocol based on RFID.
- Smartphones, digital cameras, televisions, and terminals are NFC-enabled devices.
- Credit cards, tickets, and NFC tags are examples of objects that also use NFC technology.
- An NFC tag is a chip that can store small amounts of data.
- NFC tags can be found in many different items, including business cards, wristbands, stickers, and ski lift tickets.



**Figure 9-9** NFC communication examples.

# Network Standards and Protocols

**Table 9-4 Close-distance network protocols.**

Network Protocol	Common Uses
Bluetooth	Devices communicating with one another over a short range (usually less than 30 feet/9 meters)
IrDA	Remote controls or other data transmission within close proximity
LTE	Uses radio signals to communicate data over cellular networks
NFC	Used in credit cards, smartphones, and tickets to facilitate close-range communication
RFID	Radio signals transmitted through antennas, often found in tollbooth transponders or embedded chips in animals
UWB	Low-energy radio technology for short-range, high-bandwidth communications
Wi-Fi	Hot spots and wireless home and small business networks using TCP/IP

# Network Connection Hardware

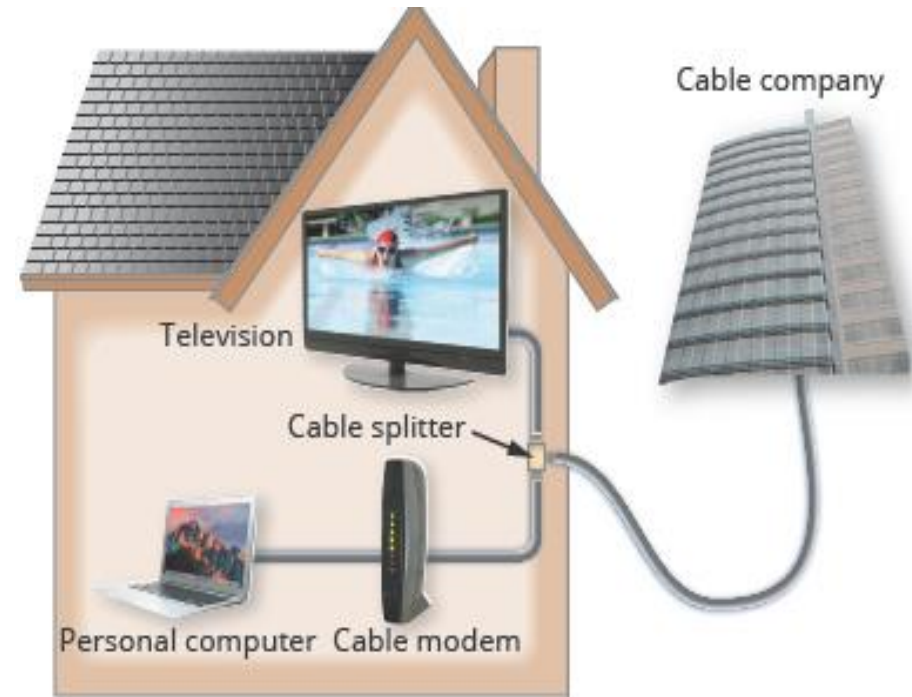
- **Nodes**, or devices on a network, can be computers, tablets, mobile phones, printers, game consoles, or smart home devices.
- **Hubs** provide a central point for network cables in a network and are used to transfer data to all devices.
- **Switches**, used more frequently than hubs, also provide a central point for network cables in a network and transfer data only to the intended recipient.
- **Routers** connect two or more networks and direct, or route, the flow of information along the networks.

# Network Connection Hardware

- A **modem** connects a sending or receiving device, such as a computer, to a communications channel, such as the Internet.
- The modem connects your network to the Internet through an ISP.
- A **digital modem**, also called a **broadband modem**, is a communications device that sends and receives data and information to and from a digital line.
- Three types of **digital modems** are **cable modems**, **DSL modems**, and **ISDN modems**.

# Network Connection Hardware

A **cable modem** uses a cable TV connection. A splitter connects one part of the cable to your cable box or device, and the other part to the cable modem.



**Figure 9-10** Typical cable modem installation.



# Network Connection Hardware

- A **DSL(Digital Subscriber Line) modem** uses standard copper telephone wiring.
- An **ISDN (Integrated Services Digital Network) modem** is a broadband modem that sends digital data and information from a computer to an ISDN line and receives digital data and information from an ISDN line.
- DSL and ISDN modems are external devices.



**Figure 9-11** Cable modem and wireless router.

# Network Connection Hardware

- A **dedicated line** is a type of always-on physical connection that is established between two communications devices.
- Businesses often use dedicated lines to connect geographically distant offices.
- Dedicated lines can be either analog or digital.
- **Multiplexing** is a process that combines multiple analog or digital signals into a single signal over a shared medium, such as a cable.
- Digital dedicated lines include cable television lines, DSL, ISDN lines, FTTP.

# Network Connection Hardware

**Table 9-5 Digital dedicated lines.**

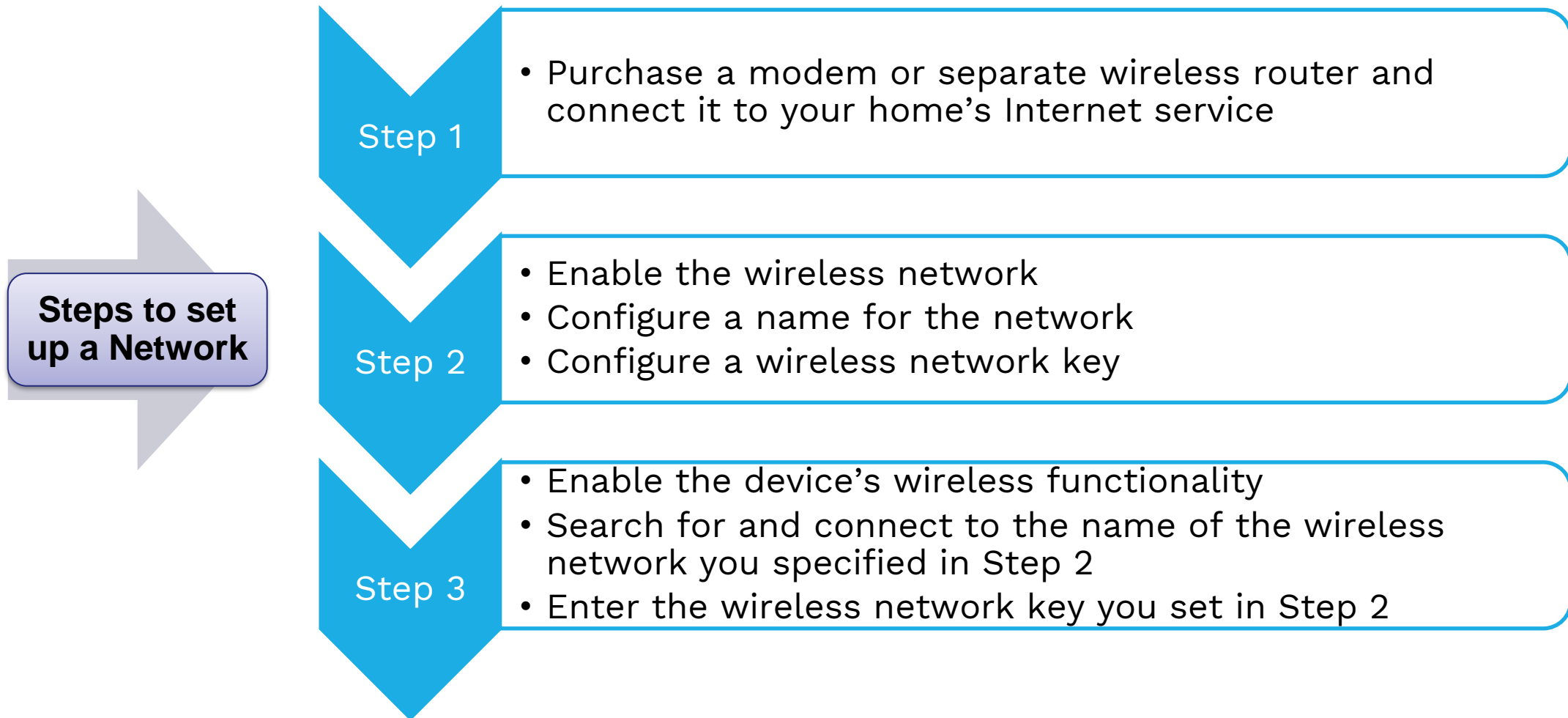
Type	Description
Cable	The cable television (CATV) network provides high-speed Internet connections. The CATV signal enters a building through a single line, usually a coaxial cable, which connects to a modem that typically attaches to your computer via an Ethernet cable.
DSL, ADSL	DSL (Digital Subscriber Line) transmits on existing standard copper phone wiring. ADSL (Asymmetric Digital Subscriber Line) is a type of DSL that supports faster downstream rates than upstream rates.
ISDN	ISDN (Integrated Services Digital Network) refers to both a circuit-switched telephone network system and a set of communication standards used to transmit data, voice, and signaling.

# Network Connection Hardware

**Table 9-5 Digital dedicated lines (continued).**

Type	Description
FTTP	FTTP (Fiber to the Premises) uses fiber-optic cable to provide extremely high-speed Internet access to a user's physical permanent location. An optical terminal at your location receives the signals and transfers them to a router connected to a computer.

# How To: Set Up a Network



# How To: Set Up a Network

- If your wireless router or wireless access point has an **antenna(s)**, extend it completely
- If you can remove the antenna(s) from your wireless router or wireless access point, replace it with a **wireless signal booster**
- Place the wireless router or wireless access point in a **central location** of your home
- Purchase a **booster (or repeater)**, which is an amplifier used to improve reception and extend the range
- Change the router if problems persist



**Figure 9-13** Wireless signal booster.

# Secure IT: Secure a Network

- Wireless Networks are easily accessible.
- It leads to several common network risks.
- Change the default password for the wireless access point, the SSID name, encryption, and a MAC address
- Keep a regular check on the number of connected devices to the wireless router

# Secure IT: Secure a Network

- **Network monitoring software** constantly assesses the status of a network and sends an email or text message, when it detects a problem.
- **Monitoring software** can measure the amount of network traffic, graph network usage, determine when a specific program uses the network, and show the bandwidth used by each computer or mobile device.
- **Packet sniffer** software monitors and logs packet traffic for later analysis.
- Hackers use **packet sniffer software** to hijack a computer.



# Secure IT: Secure a Network

Use the following steps to determine if someone is accessing a wireless network without permission:

- Sign-in to the administrative interface
- Count the number of connected devices
- Secure the network
- Enable the router's firewall and, if possible, use “stealth mode” to make the network less visible to outsiders

Thank You

